



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/716,731	11/19/2003	Michael Lee	120-139 15845ROUS02U	6311
34845 7590 01/05/2007 McGUINNESS & MANARAS LLP 125 NAGOG PARK ACTON, MA 01720			EXAMINER LEMMMA, SAMSON B	
			ART UNIT	PAPER NUMBER
			2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/716,731	Applicant(s) LEE ET AL.	
	Examiner Samson B. Lemma	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 November 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. **Claims 1-12** have been examined.

Priority

2. This application claims priority of a provisional application 60502452 filed on **09/12/2003**. Therefore, the effective filing data for the subject matter defined in the pending claims of this application is **09/12/2003**.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 1-12** are rejected are rejected under 35 U.S.C. 103(a) as being unpatentable over **Jari et al** (hereinafter refereed as **Jari**) (U.S. Patent Publication No. 2001/0020275A1) (Published on September 6, 2001) in view of **Mercer et al** (hereinafter referred to as **Mercer**) (U.S. Publication No. 2003/0018908 A1) (filed on July 23, 2001)

5. **As per claims 1-5 Jari** discloses a method for re-establishing secure communications between a node and an endpoint node including the steps of: [Abstract and paragraph 0037] (As it is described on the abstract, "When a restoration of power to the security gateway is detected following a power failure, the controller 6 retrieves the latest security association database from the memory 7 and

Art Unit: 2132

injects it into the volatile memory 5 whose contents were lost during the power failure.

The security gateway 2 **then restore secure communication with external users.**")

- **Copying**, ["retrieve" see paragraph 0013 and see "injects" on the abstract] **responsive to a reset at the node**, ["restoration of power to the node" see paragraph 0013, abstract and 0005] **a set of security associations stored in a memory** ["a volatile memory for containing a security association database comprising a plurality of security associations, see paragraph 0005] **to a working set of security associations** ["security association which is injected on the volatile memory shown on figure 1, ref. Num 5]

Furthermore Jari on paragraph 0032 discloses, the following, "the security gateway 2 controls communication between external or mobile users and the VPN 1 in accordance with the pre-negotiated security associations **in a manner which is known and which will therefore not be described further and as indicated on paragraph**". The manner, which is known, includes the **IKE SA** as described on the secondary reference on column 0024-0026]. **On paragraph 0025, the following has been described.** "To establish an IKE SA, the first 110 and second 114 gateway computers exchange digital certificates, **which have been digitally signed by a trusted third party certificate authority 115.** Thereafter, when the IKE session becomes active, the first 110 and second 114 gateway computers can establish the IPSec SA". And on paragraph 0026, the following has been described. "When this is done, the IPSec SA has been established, and the first 110 and second 114 gateway computers **store the SA in respective Security Association Databases (SADs) 116, 118.**" And nodes digitally signed **by a trusted third party are trusted nodes** and meets the limitation of "**wherein the set of security associations includes**

Art Unit: 2132

only the security associations for endpoints nodes that are trusted by the node;

Jari does not explicitly disclose

- **wherein the set of security associations includes only the security associations for endpoints nodes that are trusted by the node;**
- **Receiving, at the node, a communication from the endpoint node**
- **Determining whether a security association for the endpoint node is included in the working set of security associations;**
- **responsive to a determination that the security association for the endpoint node is in the working set of security associations, using the security association to process the communication from the endpoint node.**

However, in the field of endeavor **Mercer** discloses,

- **wherein the set of security associations includes only the security associations for endpoints nodes that are trusted by the node;**[paragraph 0025] *(If the first 110 and second 114 gateway computers already share an IKE SA, then the IPsec SA can be created fairly quickly. If not, then an IKE SA must first be established before an IPsec SA can be established. To establish an IKE SA, the first 110 and second 114 gateway computers exchange digital certificates, which have been digitally signed by a trusted third party certificate authority 115. Thereafter, when the IKE session becomes active, the first 110 and second 114 gateway computers can establish the IPsec SA.)*
- **Receiving, at the node** [paragraph 0026 and paragraph 0030] *(The second gate way computer 114/node, receives the Ipsec datagram 300, 400), a communication from the endpoint node.*[the first gateway computer 110/endpoint node, encrypts each IP datagram 200, forms a new IPsec datagram 300,400 and send it to the second gateway computer)

Art Unit: 2132

- **Determining whether a security association for the endpoint node is included in the working set of security associations;** *[paragraph 0026 and paragraph 0030], (When the second gateway computer 114 receives the IPSec datagram 300,400, which is sent from the gateway computer 110/endpoint node, it/the second gateway computer 114/node, looks up the IPSec SA in the SAD 118/working set of security associations/security association Databases, shown on figure 1, ref. Num 118)*
- **responsive to a determination that the security association for the endpoint node is in the working set of security associations, using the security association to process the communication from the endpoint node.** *(Paragraph 0026 and paragraph 0030) [It looks up the IPSec SA in its SAD 118, and this is done in order to determine that the security association for the endpoint node/gateway computer 110/ is already in the SAD 118/working set of security associations/security association Databases and once the determination is made, properly processes the datagram, and forwards it to the second individual computer workstation 112-1).*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of including only the security associations for endpoints nodes that are trusted by the node; receiving, at the node, a communication from the endpoint node; determining whether a security association for the endpoint node is included in the working set of security associations; and responsive to a determination that the security association for the endpoint node is in the working set of security associations, using the security association to process the communication from the endpoint node as per teachings of **Mercer** into the method taught by **Jari** for the purpose eliminating the need for elaborate and time consuming SAD/ security association Databases table lookup algorithms, which result in costly memory access times and complex lookup hardware. [See Mercer, paragraph 0031]

6. **As per claims 7 and 10-11 Jari discloses a network device including:**

- **Security association logic** [Abstract, figure 1, ref. 4 and paragraph 0032] *(the security gateway 2 contains a CPU 4 having a volatile memory 5 in which stored, among other things, a security association database controlling secure communication between the network and external users), coupled to the non-volatile memory, [figure 1, ref. Num 7, abstract] for applying security associations to communications received by the network device* [Abstract] *(a controller 6 periodically stores the security association database in a disk memory 7 or other nonvolatile memory)*
- **The security association logic** [Figure 1, ref. Num 4] **including:**
 - **a first memory comprising at least one entry, the entry comprising an endpoint identifier and a security association associated with the endpoint;** [paragraph 0032] *(The security gateway 2 comprises a central processing unit (CPU) 4 in the form of one or more programmable data processors controlled by a stored program. The CPU 4 includes a volatile memory 5, for example in the form of random access memory (RAM), for storing temporary values generated during operation of the CPU 4 in accordance with normal programmed data processor or computer techniques. During normal operation of the security gateway 2, the volatile memory contains, among other things, a security association database (SAD) in the form of a plurality of security associations. For example, each security association may comprise a header sequence number, encryption and authentication algorithms and parameters, and lifetime information for the security association. The security gateway 2 controls communication between external or mobile*

Art Unit: 2132

users and the VPN 1 in accordance with the pre-negotiated security associations in a manner which is known and which will therefore not be described further.) and

- **A second memory [Figure 1, ref. Num 7], storing a subset of data of the first memory [Figure 1, ref. Num 5] (The security gateway 2 contains a CPU 4 having a volatile memory 5/first memory, in which is stored, among other things, a security association database for controlling secure communications between the network and external users. A controller 6 periodically stores the security association database in a disk memory 7 or other nonvolatile memory/second memory)**

Furthermore Jari on paragraph 0032 discloses, the security gateway 2 controls communication between external or mobile users and the VPN 1 in accordance with the pre-negotiated security associations **in a manner which is known and which will therefore not be described further and as indicated on paragraph**". The manner, which is known, includes the **IKE SA** as described on the secondary reference on column 0024-0026]. **On paragraph 0025, the following has been described.** "To establish an IKE SA, the first 110 and second 114 gateway computers exchange digital certificates, **which have been digitally signed by a trusted third party certificate authority 115.** Thereafter, when the IKE session becomes active, the first 110 and second 114 gateway computers can establish the IPSec SA". And on paragraph 0026, the following has been described. "When this is done, the IPSec SA has been established, and the first 110 and second 114 gateway computers **store the SA in respective Security Association Databases (SADs) 116, 118.**" And nodes digitally signed **by a trusted third party are trusted nodes** and meets the limitation of "**wherein the set of security associations includes only the security associations for endpoints nodes that are trusted by the node;**

Jari does not explicitly disclose

A first memory comprising a list of trusted endpoints;

However, in the field of endeavor **Mercer discloses,**

- **wherein the set of security associations includes only the security associations for endpoints nodes that are trusted by the node;**[Paragraph 0025] *(If the first 110 and second 114 gateway computers already share an IKE SA, then the IPSec SA can be created fairly quickly. If not, then an IKE SA must first be established before an IPSec SA can be established. To establish an IKE SA, the first 110 and second 114 gateway computers exchange digital certificates, which have been digitally signed by a trusted third party certificate authority 115. Thereafter, when the IKE session becomes active, the first 110 and second 114 gateway computers can establish the IPSec SA.)*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of including only the security associations for endpoints nodes that are trusted by the node; as per teachings of **Mercer** into the method taught by **Jari** for the purpose of strengthening security and establishing secure communication. [See for instance, Mercer, paragraph 0012, "secure communication"]

7. **As per claim 6 the combination of Jari and Mercer discloses as claims above, furthermore Jari discloses the method further comprising in the event of a reset, copying the table of security associations to the working table of security associations.** [Abstract] *(When a restoration of power to the security gateway is detected following a power failure, the controller 6 retrieves the latest security association database from the memory 7 and injects it into the volatile memory 5 whose contents were lost during the power failure. The security gateway 2 may then restore secure communication with external users.)*

Art Unit: 2132

8. **As per claim 8** the combination of Jari and Mercer discloses as claims above, furthermore Jeri discloses the method wherein the second memory is a non-volatile memory. [figure 1, ref. Num 7, paragraphs 0033] (Abstract, non-volatile memory)
9. **As per claim 9** the combination of Jari and Mercer discloses as claims above, furthermore Jeri discloses the method further comprising, means for periodically copying the subset of data of the first memory [figure 1, ref. Num 5] to the second memory [figure 1, ref. Num 7] (paragraph 0035) (During normal operation of the security gateway 2, the current security association database in the volatile memory 5 is periodically stored in the disk memory 7 by the controller 6)
10. **As per claim 12** the combination of Jari and Mercer discloses as claims above, furthermore Jeri discloses the method further comprising, responsive to a reset at the network device, for copying contents of second memory [Figure 1, ref. Num 7, abstract] to the first memory. [figure 1, ref. Num 5, abstract] (The following is disclosed on abstract, "When a restoration of power to the security gateway is detected following a power failure, the controller 6 retrieves the latest security association database from the memory 7 and injects it into the volatile memory 5 whose contents were lost during the power failure. The security gateway 2 may then restore secure communication with external users.")

Art Unit: 2132

At last Examiner would indicate the following to show that Applicant's invention and the problem it tries to solve is the same as that of the reference used namely Jari (U.S. Patent Publication No. 2001/0020275A1)

Applicant's invention as described on Applicant's specification is trying to solve the following problem:

"Because there may be hundreds or thousands of SAs in a given communication network, in the event that a power down condition occurs in the network, and undesirably large time period is undertaken during power up to re-establish the SAs for the endpoints. For larger VPN devices, the time period for establishing connections may be up to one half hour. **Such a delay is not desirable to the consumer.**" [Page 4, lines 5-9]

Applicant Specification suggested that the above problem is solved with the following Applicant's invention.

" Node 30 shown on figure 1, includes SA logic 32, shown on figure 1 and a memory 34 shown on figure 1. [Page 6, last 2 lines of the specification and figure 1]

Memory 34 is described as "Memory devices capable of retaining its contents during a power fail, such as an external, or a non-volatile on module storage device such as an EPROM. Stored in the memory 34 is a security association (SA) table 33." **[Page 7, lines 1-4 of the applicant's specification]**

Security logic 32 is described as "SA logic 32 is shown to include a trusted nodes list 35, a security association table 36 and key generation logic 37. In one embodiment, the key generation logic operates using the Internet Key Exchange (IKE) protocol, although any other types of key exchange protocols may alternatively be used, and it is important to note that the present invention is not limited to any particular method of key generation. [Page 7, lines 11-16 of the applicant's specification]

Furthermore, as applicant indicated on page 7, lines 11 of the applicant's specification, "The memory shown on figure 1, ref. Num "34" receives the SA and identifier information from SA logic 32"

Following the above, applicant described his invention as follows.

"The list of trusted endpoints is used to select a subset of entries from the SA table

Art Unit: 2132

36 for maintenance the SA table 33 of memory 34. Periodically the entries from the SA table 36 are copied to the SA table 33. This copying may occur upon the creation or re-keying of each SA, or alternatively the table may be backed up at periodic intervals to reflect changes in network configuration. The SA logic 32 takes advantage of the fact that certain endpoints are well known to each node. These endpoints are allowed a very fast but secure method to re-establish communications with the node in the event of a power failure at the node. According to one aspect of the invention, the trusted endpoints are permitted to use the last previously negotiated security association between the node and the endpoint providing that the endpoint is one indicated in the trusted list 35. Thus, in the event of a power fail at the node 30, the contents of the SA table 36 and trusted list 35 are lost. During reboot, the values from the SA table 33 in memory 34 are copied back into the SA table 36 and trusted list 35. When the trusted endpoints next seek access to the node, they prove their identity by using the last previously negotiated SA to communicate with the node. If the SA used by the trusted endpoint corresponds to the one retrieved from memory, the endpoint is permitted to communicate immediately with the node, without having to undergo the time consuming process of re-keying the communication link. Only in the event that the SA does not match the retrieved SA from memory does the endpoint need to re-negotiate keys with the node. **As a result, considerable time is saved upon power up by permitting previously negotiated SAs to be used with trusted endpoints.** [Page 9, lines 14-page 11 of the applicant's specification]

The reference used, Namely Jari solves the same problem as indicated below,
"In the event of a power failure or other failure within the security gateway, all security associations can be lost. For example, there may be of the order of 300 such security associations and these will need to be renegotiated when the security gateway is operational again so as to re-establish secure communication. The Internet Engineering task Force (IETF) provides some specifications for restoring operation following such a failure and loss of the SAD

Art Unit: 2132

but these techniques **require a substantial amount of time before secure communication can be restored.**" [paragraph 0004]

Jari solves the above problem the as applicant's invention as described in the abstract, "An IPsec-capable node 2, such as a security gateway 2, is provided for a virtual private network 1. The security gateway 2 contains a CPU 4 having a volatile memory 5 in which is stored, among other things, a security association database for controlling secure communications between the network and external users. A controller 6 periodically stores the security association database in a disk memory 7 or other nonvolatile memory. When a restoration of power to the security gateway is detected following a power failure, the controller 6 retrieves the latest security association database from the memory 7 and injects it into the volatile memory 5 whose contents were lost during the power failure. The security gateway 2 may then restore secure communication with external users." [Abstract and paragraph 0005-0026]

Therefore Examiner as indicated above, the problem to be solved and the solution provided as applicant's invention, is the same as that of the reference on the record, namely Jari.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examine should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone

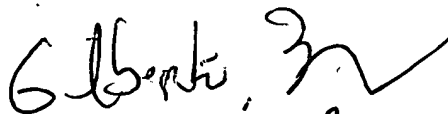
Art Unit: 2132

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S. L.
12/24/2006


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100